～真の知能を目指す人工知能～

DARKTRACE

AIを活用した
プロアクティブなサイバーセキュリティ対策

Darktraceについて
製品概要

昨今の世界情勢が不安定な中、サイバー攻撃の勢力も年々増大しており、ベンダーが保有する脅威情報に依存するだけでは、日々巧妙化するサイバー脅威への対策が十分に行えているとはいえません。

現代のサイバー防御では、攻撃の兆候を見つけ出し、深刻な被害を受ける前に防御する姿勢が求められます。

Darktraceは日々の通信をゼロから学習し、普段とは異なる挙動(時間帯・サービス・データ転送量等)の珍しさという観点から、サイバー脅威の予兆をとらえ、未然に防御することに特化した製品です。

簡単な導入

コアスイッチにミラーポートを作成し、データをDarktraceへ転送するのみで、既存のネットワーク構成の変更等面倒な手間は不要

運用負荷の軽減

AIが膨大なログから不審な通信の検知から調査まで実施し、自動で日本語のレポートを生成するため、運用者の手間を削減

便利な一括管理

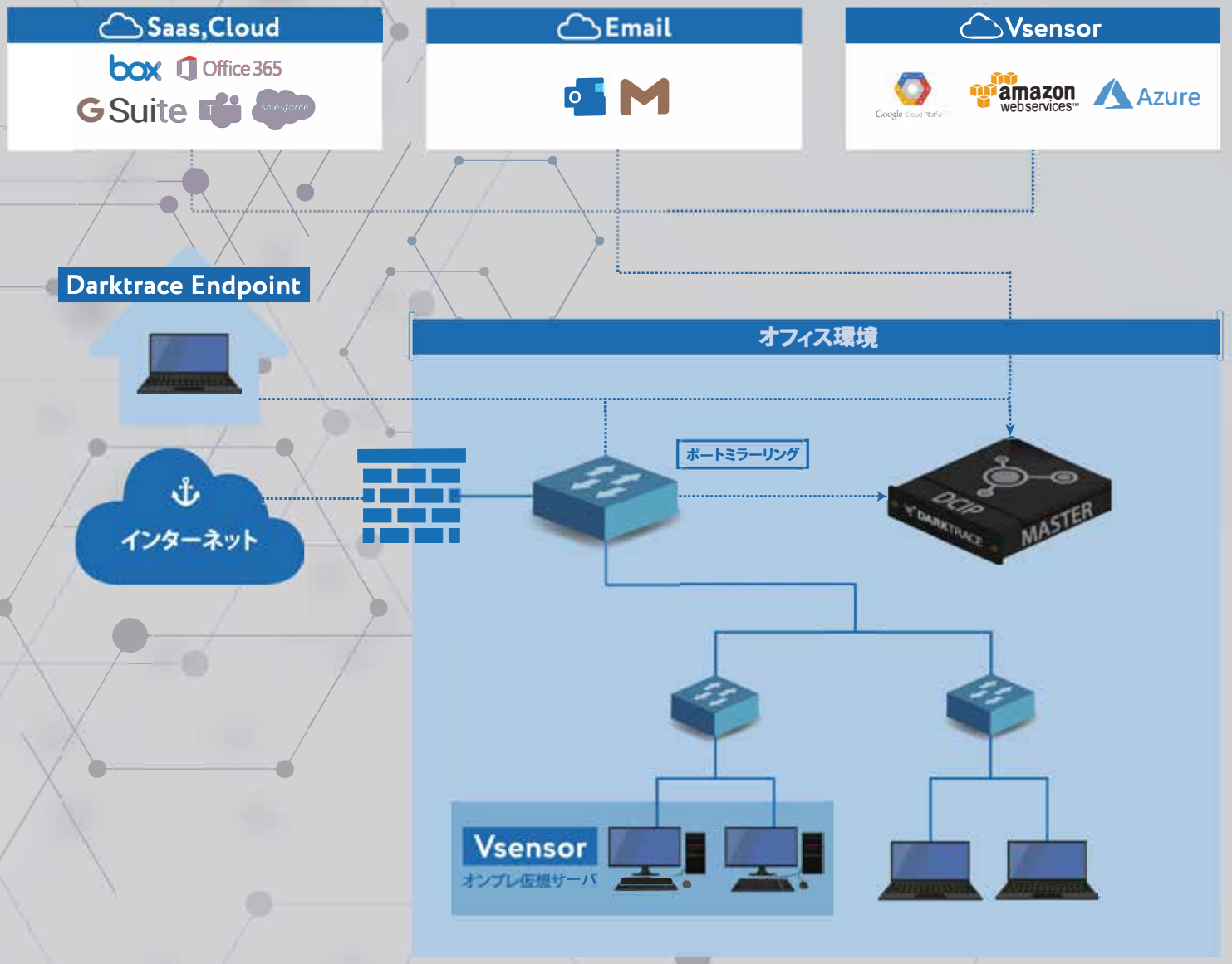
基本機能のみでなく、オプション製品も一つの統合された画面内で管理することが可能なため、管理が容易

Proof of Value : 30日間の検証

最短1時間で導入可能	3回に渡る専任のアナリストによる脅威分析	検知した脅威を週次で報告

Configuration overview
構成概要

オンプレミスなネットワーク環境では、コアスイッチからミラーリングしたデータをDarktraceの物理アプライアンスへ送り、分析・解析が行われます。また、メールやSaasアプリケーションなどのデーターも同アプライアンスへ送られ、一括で管理されます。



Schedule image
スケジュールイメージ

1	2	3
1週目〜2週目	**3週目〜4週目**	**5週目〜8週目**
事前準備 ・情報ヒアリング(NW環境の確認) ・機器手配	**機器導入** ・設置作業 ・環境学習期間(1週間)	**レポート報告会(3回)** ・脅威分析のご報告 ・運用/機能に関するQ&A

Option service
オプションサービス

Saas, Cloud
(Saasの検知・遮断)

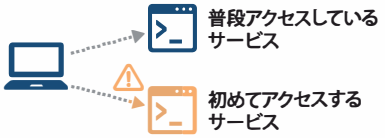
クラウド利用が普及している現代において、クラウド上で発生するサイバー脅威に対処できる手段は多くありません。
DarkTraceはクラウド上でのユーザーの行動パターンを学習し、アカウントハッキングやデータ漏洩が発生した際の被害を最小限に抑えます。

salesforce Dropbox box aws Microsoft Azure
Google Workspace Google Cloud Microsoft 365 okta

Darktrace Endpoint
(端末の検知・遮断)

独自のエージェントにより、サイバー脅威を数秒で封じ込めるPC用セキュリティソフトです。自己学習型AIによりユーザーとデバイスの動作パターンを理解し、通常とはわずかに異なる挙動や脅威にピンポイントで反応します。リモートワークのPC端末にもセキュリティが担保されます。

対応OS：Windows,macOS



Respond
(社内ネットワーク内の遮断)

脅威と認識されたインシデントに自動的に対処し、無害化・封じ込めを行う機能です。
DarkTraceが学習した行動パターンから外れたユーザー、デバイス、ネットワークの動きをいち早く検知し、マルウェアや情報漏洩を食い止めます。
未知なサイバー脅威に対しても迅速な処理を実現可能です。

防御例 ランサムウェア 内部情報漏洩 違反

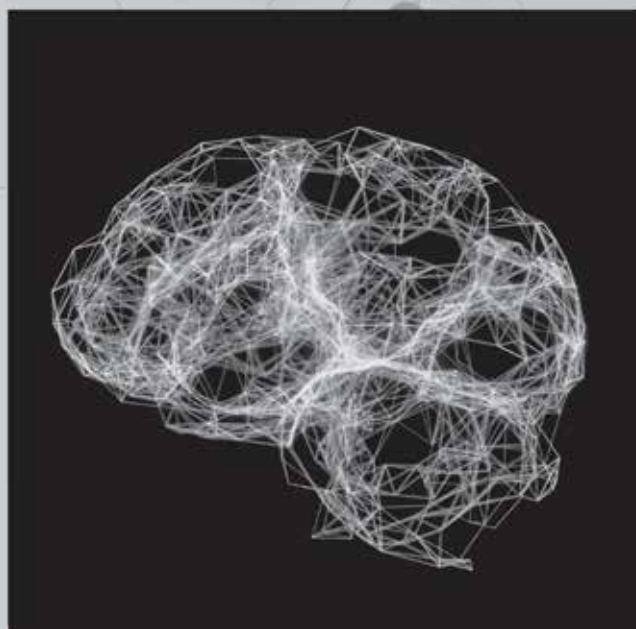
Email
(メールの検知・遮断)

ユーザーが行っている普段のメールのやりとりを学習し、通常とは異なるメールを受信した際に脅威を防ぎます。
一見無害のようにみえる電子メールでも、それが悪意あるメールである可能性を明らかにし、処理されることで、巧妙なりすましメールや高度なフィッシングに対しての攻撃の無力化を実現します。

対象メールサービス：Microsoft365、Gmail

Company
会社概要

ダークトレースは、英国ケンブリッジで2013年に設立された、人工知能のアルゴリズムを応用して開発された自己学習型のプラットフォームを展開しています。
AIを駆使してサイバーセキュリティで業界をリードする企業で、世界各国で7,400以上のお客様に導入実績があり、クラウド、Eメール、SaaS、従来型ネットワーク、IoTデバイス、エンドポイント、産業用制御システムを含む組織のデジタル環境を全域にわたり網羅的に防御しています。



Cyber AI Analyst
サイバーAIアナリストについて

アラートを自動的に調査・分析をし、レポートを作成
人間のアナリストが
脅威を調査・分析する際の思考パターンを機械学習

脅威内容を自動的にレポート作成

Darktrace Enterprise Immune System

機器スペック表

	DCIP-S	DCIP-M	DCIP-X2-11G	DCIP-Z
形状	1 Uハーフラックマウント型	1U ラックマウント型	2U ラックマウント型	2U ラックマウント型
寸法(cm)	44cm x 37cm x 4.4cm	44cm x 74.5cm x 4.4cm	44cm x 74.5cm x 8.8cm	44cm x 74.5cm x 8.8cm
重量 (kg)	6 kg	15 kg	23 kg	23 kg
インターフェース管理ポート	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T
リモート管理ポート	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T
分析用ポート	3 x 10/100/1000 BASE-T	3 x 10/100/1000 BASE-T	1 x 10/100/1000 BASE-T 2 x 10 GBASE-T	1 x 10/100/1000 BASE-T 2 x 10 GBASE-T
SFP+分析ポート	—	2 x 10Gbe/1Gbe SFP+	2 x 10Gbe/1Gbe SFP+	2 x 10Gbe/1Gbe SFP+
最大スループット	～ 300 Mbps	～ 2Gbp	～ 5Gbps	～ 5Gbps
最大管理端末数	最大1000台	最大8000台	最大36000台	最大50000台
最大接続数/分	2,000	50,000	100,000	250,000
電源供給	シングル 260W IEC 13C 120/240V	デュアル750W IEC 13C 120/240V	デュアル1110W IEC 13C 120/240V	デュアル1110W IEC 13C 120/240V
消費電力	Idle 26 W- Max 105 W	Idle 120 W- Max 418 W	Idle: 128 W- Max 426 W	Idle: 128 W- Max 426 W
対応拡張モジュール	拡張モデル1機種に対応可能。 • 2-port 1G/10G SFP+ • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	拡張モデル1機種に対応可能。 • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1G RJ45 1000 BASE-T	拡張モデル3機種に対応可能。 • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1GRJ45 1000 BASE-T	拡張モデル3機種に対応可能。 • 2-port 1G/10G SFP+ • 2-port 10G RJ45 10000 BASE-T • 2-port 1G RJ45 1000 BASE-T • 4-port 1GRJ45 1000 BASE-T
安全認証	UL 60950-CSA 60950, EN 60950, IEC 60950 CB Certicate & Report, IEC 60			
EMI認証	FCC Part 15, Class A (CFR 47) (USA), ICES-003 Class			

vSensorの要求スペック

仮想マシンOS：Ubuntu 20.04 Focal (v5.1 and above)

※vSensorの処理能力はCPU速度と解析トラフィックの内容によって異なるため、本表指定のスペックは参考情報となります。

解析対象デバイス数	50	100	200	400	800
帯域幅合計	100 Mbps	250 Mbps	500 Mbps	1000 Mbps	2000 Mbps
仮想CPU	2	4	8	16	32
仮想メモリ	8 GB	16 GB	32 GB	64 GB	128 GB
仮想ストレージ	50 GB	100 GB	200 GB	400 GB	800 GB

Darktrace Endpointの技術的要件・使用容量

使用容量	メモリ使用量	1G
	ディスク使用量	50MB
対応OS	Windows 8.1+, Windows Server 2012R2+, MacOS 10.14+, Ubuntu 18.04+, RHEL/Centos 7+, Debian 9+, openSUSE 15.0+/SUSE Linux Enterprise 12.4+, Fedora (maintained versions)	

株式会社ピーエスアイ

https://www.psi.co.jp/

本社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル4F
Tel:03-3357-9980 Fax:03-5360-4488

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原4ー1ー4 KDX新大阪ビル9F
Tel:06-6151-4034 Fax:06-6151-4035

福岡営業所
〒810-0001 福岡県福岡市中央区天神3-4-5 ピエトロビル4F
Tel:092-731-1238

名古屋営業所
〒460-0003 愛知県名古屋市中区錦2丁目9ー27 NMF名古屋伏見ビル8F-A
Tel:052-217-8810